Amendments to the Drawings:

The attached sheet of drawings includes changes to Fig. 4. This sheet, which includes Fig. 4, replaces the original sheet including Fig. 4. In Figure 4, steps 420 and 422 have been added to avoid an infinite loop.

Attachment: Replacement Sheet

REMARKS

The Examiner has objected to the drawings. Applicant has amended Figure 4 as suggested by the Examiner and submitted herewith a copy of the amended replacement drawing sheet. Further, the specification has been amended to conform to Figure 4, as amended per the request of the Examiner.

The Examiner has stated that the title of the invention is not descriptive. A new title has been entered, per the request of the Examiner.

The Examiner has rejected Claims 1-36 under 35 U.S.C. 102(b) as being clearly anticipated by Drake (U.S. Patent No. 6,006,328). Applicant respectfully disagrees with such rejection, especially in view of the amendments made hereinabove to each of the independent claims. Specifically, applicant has amended each of the independent claims to include the subject matter of dependent Claims 4 and 5 et al.

With respect to each of the independent claims, the Examiner has relied on the following excerpt from Drake to make a prior art showing of applicant's claimed "interrupting execution of a process that has been loaded for execution, wherein the execution of the process is interrupted by an anti-malware program" (see each of the independent claims, as amended).

> "As hereinbefore described, it is desirable to detect tampering, since this may lead to the reduction of software security.
>
> This can be achieved with the use of code which is protected from disassembly and examination through obfuscation and encryption, which re-reads its own external-image and compares it with its known memory image or precalculated check-data to detect hot-patching (ie. the modification of software sometime after it has been loaded from disk, but (usually) before execution of the modified section has commenced).
>
> Additionally, **the software can scan the memory image of itself** one or more times, or continuously, to ensure that unexpected alterations do not occur." (Col. 6, lines 6-20-emphasis added)
>
> "When tracing software, instructions are usually executed one-at-a-time in order for the user to understand their operation. Many

> system interrupts must occur regularly (eg: timer and memory refresh operations), so debuggers usually do not disable interrupts even when they encounter an interrupt-disabling instruction. If timers and the like are re-vectored in two separate stages, any timer (etc) interrupt occurring in between the two stages will fail, and usually crash the computer. Further, interrupts can be disabled or enabled using obscure means (with flag-altering instructions for example) to hamper tracing.
>
> Discretely testing the status of disabled or enabled system facilities (eg. interrupts, keyboard, vector-pointers) to ensure that a debug environment has not altered or by-passed them will seriously hamper tracing also." (Col. 7, lines 21-35)
>
> "Scanning the command environment and the execution instruction can detect the execution of software by unusual means. Searching for "DEBUG" in the command line, or scanning memory for known debuggers for example will detect tracing. Additional, by detecting which operating system process initiated the load of the software, unexpected processes (eg: debuggers) can be detected.
>
> Monitoring system buffers (eg: the key board memory buffer) or hardware (eg: the keyboard circuitry and internal buffers) for unexpected use (eg: keyboard input and processing is occurring when the software is not requesting it) will also detect debuggers, which usually rely in part on system functions in order to operate." (Col. 7, lines 53-65)

Applicant respectfully asserts that the interrupts in the above excerpts are merely initiated by normal system operation, and are not prompted by an anti-malware program, as presently claimed by applicant (see amended independent claims). In addition, Drake simply discloses that "the software can scan the memory image of itself" (see emphasized excerpt above) which clearly does not meet any sort of anti-malware program for interrupting the execution of a process, in the context claimed by applicant.

With respect to dependent Claim 5 et al., the subject matter of which is presently incorporated into each of the independent claims, the Examiner has relied on Col. 6, lines 6-23 of Drake to make a prior art showing of applicant's claimed "interrupting execution of the process when the process accesses at last one file that is not needed to perform decryption, decompression, or unpacking." However, after carefully reviewing such excerpt, along with the entire Drake reference, it is clear that Drake does not teach "interrupting execution of the process when the process accesses at last one file that is <u>not</u>

needed to perform decryption, decompression, or unpacking" (emphasis added), in the manner claimed by applicant.

Despite this deficiency in the prior art, and in the spirit of expediting the prosecution of the instant application, applicant has amended each of the independent claims to require a technique "wherein the at least one file is selected from the group consisting of a system library file, an executable file not related to the process, and a data file not related to the process." Again, applicant respectfully asserts that the Drake reference simply does not meet such specific claim language.

Additionally, applicant has also amended each of the independent claims to require "interrupting execution of the process when the process accesses at least one file that is not needed to perform decryption, decompression, or unpacking, after decryption, decompression, or unpacking, where encryption, compression, or packing is carried out by an entity separate from the anti-malware program" (emphasis added). Applicant respectfully asserts that, in Drake, the anti-malware obfuscates or encrypts various files or processes, while applicant teaches and claims that a separate entity performs the encryption, compression or packing. Further, applicant's amended claims require that the interrupting occur "after decryption, decompression, or unpacking."

The Examiner is reminded that a claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described in a single prior art reference. *Verdegaal Bros. v. Union Oil Co. Of California*, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987). Moreover, the identical invention must be shown in as complete detail as contained in the claim. *Richardson v. Suzuki Motor Co.*868 F.2d 1226, 1236, 9USPQ2d 1913, 1920 (Fed. Cir. 1989). The elements must be arranged as required by the claim.

This criterion has simply not been met by the Drake reference, especially in view of the amendments made hereinabove. A notice of allowance or a specific prior art

showing of each of the foregoing claimed features, in combination with the remaining claimed features, is respectfully requested.

Applicant further notes that the prior art is also deficient with respect to the dependent claims. For example, with respect to dependent Claim 12 et al., the Examiner has relied on Col. 1, line 56-Col. 2, line 62 and Col. 3, lines 33-67 to make a prior art showing of applicant's claimed "scanning the process for a malware before execution of the process." Applicant respectfully asserts that such excerpts merely suggest different ways of introducing rogue software into a system and providing computer software with enhanced security features, but not that any sort of process is scanned before the execution thereof, in the manner claimed by applicant.

Again, a notice of allowance or a specific prior art showing of all of the claim limitations, in the context of the remaining elements, is respectfully requested.

Still yet, applicant brings to the Examiner's attention the subject matter of new Claims 37-39 below, which are added for full consideration:

"terminating the process if malware is found before the execution of the process" (see Claim 37);

"wherein the terminating further comprises the step of:
performing anti-virus processing on the process if malware is found;
wherein the anti-virus processing includes at least one of quarantining, cleaning, and deleting files storing the loaded code" (see Claim 38); and

"wherein the interrupting of the execution of the process is performed before any malware in the loaded code has a chance to perform any malicious or unauthorized actions" (see Claim 39).

Thus, all of the independent claims are deemed allowable. Moreover, the remaining dependent claims are further deemed allowable, in view of their dependence on such independent claims. The Applicant respectfully requests reconsideration of this application and early issuance of the Notice of Allowance.

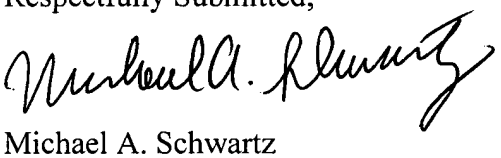
Additional Fees:

The Commissioner is hereby authorized to charge any insufficient fees or credit any overpayment associated with this application to Deposit Account No. 19-5127 (19903.0011).

Conclusion

In view of the foregoing, all of the Examiner's rejections to the claims are believed to be overcome. The Applicants respectfully request reconsideration and issuance of a Notice of Allowance for all the claims remaining in the application. Should the Examiner feel further communication would facilitate prosecution, he is urged to call the undersigned at the phone number provided below.

Respectfully Submitted,



Michael A. Schwartz
Reg. No. 40,161

Dated: June 29, 2005

Swidler Berlin, LLP
3000 K Street, N.W., Suite 300
Washington, D.C. 20007
(202) 424-7500